

CLAIMS:

1. A method of transferring a data file having a file name from a first computer operated by a first user to a second computer operated by a second user, under control of a third computer, comprising the steps of:
 - i) in the first computer, the first user selecting a data file for transfer and establishing a communications link with the third computer;
 - ii) verifying an identity of the first user to the third computer by way of verification communications between the first and third computers;
 - iii) in the first computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and then transmitting the executable file containing the wrapped or encrypted data file directly to the second computer together with first user identification information and the file name of the data file;
 - iv) transmitting the file name of the data file from the first computer to the third computer, together with first user identification information and the unique key code;
 - v) in the second computer, upon receipt of the executable file containing the wrapped or encrypted data file and upon attempted access thereto by the second user, establishing a communications link with the third computer;
 - vi) verifying an identity of the second user to the third computer by way of verification communications between the second and third computers;
 - vii) upon successful verification of the identity of the second user, transmitting the file name of the data file from the second computer to the third computer with a request for the unique key code; and

viii) transmitting the unique key code from the third computer to the second computer so as to cause the executable file to unwrap or decrypt the data file and to allow access thereto in the second computer by the second user.

2. A method according to claim 1, wherein the identity of the first user is verified in step ii) above by way of the first user applying a first user mask code to a pseudo-random security string in the first computer so as to generate a first user volatile identification code, the first user transmitting the first user volatile identification code to the third computer and the third computer comparing the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random string in the third computer, identity verification taking place when the first user volatile identification code and the first check volatile identification codes are found to match each other.

3. A method according to claim 1, wherein the identity of the second user is verified in step vi) above by way of the second user applying a second user mask code to a pseudo-random security string in the second computer so as to generate a second user volatile identification code, the second user transmitting the second user volatile identification code to the third computer and the third computer comparing the second user volatile identification code with a second check volatile identification code obtained by applying the second user mask code to the pseudo-random string in the third computer, identity verification taking place when the second user volatile identification code and the second check volatile identification codes are found to match each other.

4. A method according to claim 3, wherein the first user mask code and the second user mask code are applied to the same pseudo-random security string.

5. A method according to claim 4, wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the first computer to the second computer.
6. A method according to claim 4, wherein the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the third computer to the second computer.
7. A method according to claim 3, wherein the first user mask code and the second user mask code are applied to different pseudo-random security strings.
8. A method according to claim 1, wherein the identity of the first or second user is verified, respectively, through said first or second computer by way of a secure user code entry interface for entry of a user mask code by way of the computer and a display; wherein:
- i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display; and
 - ii) a random run on time is added to said response time to extend said at least one active display.
9. A method according to claim 2, wherein:
- i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.);

ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.); and

iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code.

10. A method according to claim 1, wherein the third computer maintains a record of transactions between the first, second and third computers so as to permit an audit trail to be established.

11. A method according to claim 2, wherein the first and/or second user volatile identification codes are stored as digital signatures in the third computer in combination with the associated pseudo-random security string.

12. A method of transferring a data file to a first computer from a second computer, the method comprising the steps of:

- i) establishing a communications link between the first and second computers;
- ii) selecting, by way of the first computer, a data file for transfer from the second computer;
- iii) in the second computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and then transmitting the executable file containing the wrapped or encrypted data file to the first computer;

- iv) verifying an identity of a user of the first computer to the second computer by way of verification communications between the first and second computers;
- v) upon successful verification of the user of the first computer, transmitting the unique key code to the first computer.

13. A method according to claim 12, wherein the identity of the first user is verified in step iv) above by way of the first user applying a first user mask code to a pseudo-random security string in the first computer so as to generate a first user volatile identification code, the first user transmitting the first user volatile identification code to the second computer and the second computer comparing the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random string in the second computer, identity verification taking place when the first user volatile identification code and the first check volatile identification codes are found to match each other.

14. A method according to claim 12, wherein the identity of the first user is verified through said first computer by way of a secure user code entry interface for entry of a user mask code by way of the computer and a display; wherein:

- i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display illuminates or highlights at least one display digit within said active display and said user enters said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display; and
- ii) a random run on time is added to said response time to extend said at least one active display.

15. A method according to claim 13 or any claim depending therefrom, wherein:

- i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.);
- ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.); and
- iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code.

16. A method of transferring a data file to a first computer having a first telecommunications address from a second computer having a second telecommunications address, comprising the steps of:

- i) transmitting a request for the data file from the first computer to the second computer, the request including data identifying the data file and the first telecommunications address;
- ii) in the second computer, wrapping or encrypting the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code;
- iii) assigning a unique identification string to the executable file in the second computer, the unique identification string being further associated in the second computer with the first telecommunications address;

- iv) transmitting the executable file (containing the data file) and the unique identification string from the second computer to the first computer;
- v) causing a message to be displayed by the first computer showing the unique identification string and requesting a user to call a predetermined telephone number from a telephone operated by the user;
- vi) receiving a telephone call from the telephone operated by the user, determining its telephone number and receiving the unique identification string from the user;
- vii) in the second computer, generating a pseudo-random string, associating the pseudo-random string with the unique identification string and the telephone number of the telephone operated by the user, and transmitting the pseudo-random string to the telephone operated by the user;
- viii) applying a mask code, known to the user and to the second computer, to the pseudo-random identification string so as to generate a volatile identification code in accordance with predetermined rules;
- ix) transmitting the volatile identification code to the second computer, either from the telephone operated by the user in which case the volatile identification code is transmitted together with the telephone number of the telephone operated by the user, or from the first computer in which case the volatile identification code is transmitted together with the first telecommunications address, the telephone number or the first telecommunications address respectively serving to identify the first computer, the user and the executable file;
- x) in the second computer, checking that the volatile identification code matches a volatile identification code generated therein by applying the mask code to the pseudo-random string and, if so;

xi) transmitting the key code to the first computer so as to enable the executable file to unwrap or decrypt the data file and to install this on the first computer.

17. A secure data transfer system comprising a first computer operated by a first user, a second computer operated by a second user and a third computer, the system being adapted to transfer a data file having a file name from the first computer to the second computer under control of the third computer, in which:

- i) the first computer is adapted to establish a communications link with the third computer upon selection by the first user of a data file for transfer;
- ii) the first and third computers are adapted to verify an identity of the first user to the third computer by way of verification communications between the first computer and the third computer;
- iii) the first computer is adapted to wrap or encrypt the data file within an executable file adapted to unwrap or decrypt the data file only upon activation by a unique key code, and to transmit the executable file containing the wrapped or encrypted data file directly to the second computer together with first user identification information and the file name of the data file;
- iv) the first computer is adapted to transmit the file name of the data file from the first computer to the third computer, together with first user identification information and the unique key code;
- v) the second computer is adapted, upon receipt of the executable file containing the wrapped or encrypted data file and upon attempted access thereto by the second user, to establish a communications link with the third computer;

vi) the second and third computers are adapted to verify an identity of the second user to the third computer by way of verification communications between the second computer and the third computer;

vii) the second computer is adapted, upon successful verification of the identity of the second user, to transmit the file name of the data file from the second computer to the third computer with a request for the unique key code; and

viii) the third computer is adapted to transmit the unique key code from the third computer to the second computer so as to cause the executable file to unwrap or decrypt the data file and to allow access thereto in the second computer by the second user.

18. A system as claimed in claim 17, adapted such that the identity of the first user is verified in step ii) above by way of the first user applying a first user mask code to a pseudo-random security string in the first computer so as to generate a first user volatile identification code, the first user transmitting the first user volatile identification code to the third computer and the third computer comparing the first user volatile identification code with a first check volatile identification code obtained by applying the first user mask code to the pseudo-random string in the third computer, identity verification taking place when the first user volatile identification code and the first check volatile identification codes are found to match each other.

19. A system as claimed in claim 18, adapted such that the identity of the second user is verified in step vi) above by way of the second user applying a second user mask code to a pseudo-random security string in the second computer so as to generate a second user volatile identification code, the second user transmitting the second user volatile identification code to the third computer and the third computer comparing the second user volatile identification code with a second check volatile identification code obtained by applying the second user mask code to the pseudo-random string in the third computer, identity verification taking place when the

second user volatile identification code and the second check volatile identification codes are found to match each other.

20. A system as claimed in claim 19, adapted such that the first user mask code and the second user mask code are applied to the same pseudo-random security string.

21. A system as claimed in claim 20, adapted such that the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the first computer to the second computer.

22. A system as claimed in claim 20, adapted such that the pseudo-random string is generated by the third computer and transmitted firstly to the first computer and then from the third computer to the second computer.

23. A system as claimed in claim 19, adapted such that the first user mask code and the second user mask code are applied to different pseudo-random security strings.

24. A system as claimed in claim 17, adapted such that the identity of the first or second user is verified, respectively, through said first or second computer by way of a secure user code entry interface for entry of a user mask code by way of the computer and a display; wherein:

i) said secure user code entry interface contains at least one active display for entry of at least one digit of said user mask code by the user; wherein said active display is adapted to illuminate or highlight at least one display digit within said active display and said interface is adapted to allow said user to enter said at least one digit of said user mask code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user mask code is illuminated or highlighted in said active display; and

ii) a random run on time is added to said response time to extend said at least one active display.

25. A system as claimed in claim 18, wherein:

i) the pseudo-random string comprises a first linear array of characters, each character having a given numerical position in the first array (first, second, third etc.);

ii) the mask code comprises a second linear array of numbers, each number having a given numerical position in the second array (first, second, third etc.); and

iii) the volatile identification code is generated by applying the mask code to the pseudo-random string so as sequentially to select numerical positions in the first array on the basis of the numbers in the second array, taken in positional order, and to return the characters thereby selected from the first array in sequence so as to form a third linear array, this third linear array forming the volatile identification code.

26. A system as claimed in claim 17, wherein the third computer is adapted to maintain a record of transactions between the first, second and third computers so as to permit an audit trail to be established.

27. A system as claimed in claim 18, wherein the third computer is adapted to store said first and/or second user volatile identification codes as digital signatures in combination with the associated pseudo-random security string.